AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America
v.

RASHEE MACKMORE,
PRECIOUS KELLY, and
RASHEE WASHINGTON,

Defendant(s)

Case No. 2:24-MJ-07506-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

As described in the accompanying attachment, defendant violated the following statutes:

Code Section	*Offense Description*
18 U.S.C. §§ 1343, 1344, 1349, 1028A	Conspiracy to Commit Wire and Bank Fraud, Aggravated Identity Theft

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s Nickolaus Jones
Complainant's signature

Nickolaus Jones, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: December 20, 2024

Judge's signature

City and state: Los Angeles, California

Hon. Maria A. Audero, U.S. Magistrate Judge
Printed name and title

AUSA Andrew Brown, 11th Floor, x0102

Complaint Attachment

Count One, 18 U.S.C. § 1349

Beginning in or before 2018, and continuing through the present, in Los Angeles County, within the Central District of California, and elsewhere, defendants RASHEE MACKMORE, PRECIOUS KELLY, and RASHEE WASHINGTON (collectively, "Defendants"), and others, conspired to commit wire and bank fraud, in violation of Title 18, United States Code, Sections 1343 and 1344. The objects of the conspiracy were carried out, and to be carried out, in substance, as follows: Defendants would steal the identities of victims and apply for credit in their names. Defendants would counterfeit identity documents so that they and their co-conspirators could better impersonate their victims. Defendants would also counterfeit credit and debit cards and checks, and supply them to their co-conspirators. Defendants and their co-conspirators used interstate wires to defraud their victims throughout this conspiracy, including U.S. Bank, J.P. Morgan Chase Bank, and Bank of America, which were then federally insured.

Count Two, 18 U.S.C. § 1028A

Beginning in or before 2018, and continuing through the present, in Los Angeles County, within the Central District of California, and elsewhere, defendants RASHEE MACKMORE, PRECIOUS KELLY, and RASHEE WASHINGTON knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person during and in relation to a felony violation of Title 18, United States Code, Section 1349, Conspiracy to Commit Wire and Bank Fraud, as charged in Count One, knowing that the means of identification belonged to another actual person.

AFFIDAVIT

I, Nickolaus Jones, being duly sworn, do hereby depose and say:

1. I am a Special Agent ("SA") with United States Immigration and Customs Enforcement, Homeland Security Investigations (HSI) and have been so employed since June 2004. I am currently assigned to HSI's San Diego Cyber Intrusion Group. I have a Bachelor of Arts Degree in Political Science from the University of California, Los Angeles. I am a graduate of the Criminal Investigator Training Program and the Immigration and Customs Enforcement Special Agent Training Program, at the Federal Law Enforcement Training Center. As a member of the Cyber Intrusion Group, I investigate cybercrimes, such as computer intrusions (commonly referred to as hacking), access device fraud, fraud in connection with identification documents, and Internet fraud and financial crimes. Based on my training and experience, I am familiar with the manner in which persons engaged in access device fraud; the manner in which access devices crimes are perpetrated; certain techniques, methods, or practices commonly used by persons engaged in access device fraud activity; and indicia of cybercrime activity. This training and experience form the basis for opinions I express below.

SEEKING ARREST WARRANTS AND COMPLAINT

2. This affidavit is made in support of an application for a criminal complaint and arrest warrant for RASHEE MACKMORE ("MACKMORE"), his fiancée PRECIOUS KELLY ("KELLY"), and his

adult son RASHEE WASHINGTON ("WASHINGTON"), for violations of Title 18, United States Code, Sections 1349, 1343, 1344, and 1028A (conspiracy to commit wire and bank fraud, and aggravated identity theft).

PROBABLE CAUSE

Summary of Investigation

3. An Undercover Agent ("UCA") contacted Rashee Mackmore ("MACKMORE"), telephonically, to purchase fraudulent identifications and fraudulent identification authentication features. Via a text messaging conversation with MACKMORE, MACKMORE confirmed with the UCA that he sold fraudulent identifications and identification authentication features. MACKMORE has also received shipments of fraudulent identification making equipment. The investigation further showed that MACKMORE had a criminal history which included identity theft, counterfeiting, and forgery, and that he has engaged in various financial crimes involving fraudulent identifications. In January 2024, a search warrant was served on MACKMORE's residence, resulting in the seizure of fraudulent identifications and identification making equipment. MACKMORE confessed. I told him he would need to retain defense counsel to negotiate a guilty plea, and he indicated he would. In May 2024, MACKMORE stopped responding to my phone calls and text messages, and moved apartments, not providing any forwarding information.

MACKMORE Repeatedly Received Proceeds of Fraud

4. Bank and financial institution records show that MACKMORE has repeatedly received fraud proceeds:

a. On April 21, 2021, A Bank of the West ("BOTW") checking account in the name of Keandre China ("CHINA") received an incoming transfer for $20,342 from Harvest Small Business Finance, a direct lender of the Small Business Administration (SBA) Economic Injury Disaster Loan ("EIDL") program. CHINA was listed as the beneficiary of the transfer. However, CHINA could not provide any documentation regarding a business or applying for the loan. Also on April 21, 2021, CHINA began withdrawing and transferring all of the funds from the account, to include sending a $2,500 Zelle Payment to MACKMORE.

b. On December 15 and 19, 2022, two counterfeit checks, for a combined value of $7,800 were deposited into a U.S. Bank ("USB"), account in the name of Eric Evans. Immediately thereafter the funds began to be withdrawn from the account by cash withdraws and electronic transfers, to include two electronic Zelle transfers for $80 on December 28, 2022, and January 23, 2023, to MACKMORE.

c. JP Morgan Chase Bank closed Credit Card xxxxxxxxxxxx6198 ("6198") for identity theft. From May 1, 2022, through December 20, 2022, fifty-six fraudulent transactions totaling $17,728.39, were charged to 6198. JP Morgan's fraud investigation showed that 6198 was opened using the account holder's information, but without their consent (identity theft). JP Morgan's fraud investigation also yielded merchant documents which identified MACKMORE and Precious Kelly ("KELLY")

as suspects. (As described below, KELLY is MACKMORE's live-in girlfriend.)

d. MACKMORE had been the signer on three personal Bank of America accounts, including one which was a joint personal checking account with KELLY. From September 16, 2019, to October 7, 2020, the accounts had cash deposits totaling approximately $138,739. Bank records reflect that both MACKMORE and KELLY claim to be an "Executive" at "Computer Care Systems." A google search for "Computer Care Systems" and "MACKMORE" returned no results, however. Further, while there are corporate entities associated with MACKMORE, according to Opencorporates which collects such data, they are both inactive and were in other fields (trucking and entertainment). Based on my training and experience, the cash deposits are not indicative of income from employment as an executive at a computer care systems business.

MACKMORE Is Linked to Cryptocurrency Wallets that Conduct Transactions on the Dark Web

5. Financial institution records show from December 7, 2018, to August 21, 2022, MACKMORE was associated with suspicious virtual currency movements. Eleven Bitcoin Depot Virtual Currency ATM accounts were all linked by sending funds to the same virtual wallet. One of the eleven accounts belonged to MACKMORE. Some of the linked accounts used suspected fraudulent identifications. The accounts also sent funds to various high-risk marketplaces, such as PinPays, GetBette, JokerStash, BriansClub, UniCCShop, FeShop, BigFat, Slillpp,

WorldMarket, and Robocheck. In my training and experience, these sites sell stolen identities, stolen credit card information, and equipment useful to identity thieves. One of the linked Bitcoin Depot accounts, listed MACKMORE's true name.

MACKMORE Has Many Convictions, Including for Fraud

6. I reviewed MACKMORE's criminal history, which shows more than a dozen convictions. On October 8, 2009, MACKMORE was convicted of organizing a financial criminal enterprise and sentenced to six years in prison. He also has arrests for counterfeiting and identity theft in 2008.

MACKMORE's Had Received Under Aliases Supplies Used by Counterfeiters

7. My further queries of law enforcement databases identified various residential addresses for MACKMORE.

8. I conducted queries and analysis of importation records related to MACKMORE and his addresses, finding the following:

a. Only one person, in the last year, "Matthew Quinn," had received international shipments at MACKMORE's search warrant address. The shipments included: 9/17/23, "hot melt machine glue," from a shipper in China; 7/22/23, "plastic household articles," from a shipper in China; and 5/9/23, "PLASTIC A4 SIZE LAMINATED SHEETS," from a shipper in China. Based on my training and experience I know that hot melt machine glue and plastic A4 size laminated sheets, are both materials that can be used to manufacture fraudulent identifications.

b. MACKMORE had received one international shipment at an address in Chicago, in 2022, listing his phone number as 773-808-4582. The name "Alexandra Alomari" had also used MACKMORE's same phone number, 773-808-4582, to receive international shipments at MACKMORE's previous address, 1111 Wilshire Blvd, Apt 606, Los Angeles, CA. These included two shipments on December 2 and 15, 2020, shipped from Dongguan Piaoliang Shi Ye Co Ltd ("DONGGU"), in China. They were manifested as: "LABEL SAMPLE;" with a weight of .5 kilograms. I conducted additional queries and analysis of importations from DONGGU. I found that on February 9, 2021, DONGGU had sent another shipment manifested as "Label Sample," with a weight of .5 kilograms, to a subject in Georgia. U.S. Custom and Border Protection inspected that package, revealing that it contained thirty counterfeit Driver's license holographic security seals, as used in manufacturing fraudulent driver licenses.

9. I conducted further queries of law enforcement databases regarding MACKMORE and his addresses. My queries revealed the following pertinent information:

a. "Larry Alexandra," "Alexandra Alomari," and MACKMORE all have resided at 1111 Wilshire Blvd, Apt 606, Los Angeles, CA, as well as, more recently, MACKMORE's address which we searched.

b. "Larry Alexandra" was listed as a subscriber of MACKMORE's other phone, 217-994-7002, and residing at MACKMORE's search warrant address.

10. My queries of "Larry Alexandra" and "Alexandra Alomari" showed that both are associated with social security numbers issued out of sequence. Furthermore, I was not able to locate any driver's licenses for either "Larry Alexandra" or "Alexandra Alomari." I also conducted queries of "Matthew Quinn" residing at MACKMORE's search warrant address, and I was not able to locate any records of an individual by that name residing there. Based on my training and experience, persons with social security numbers issued out of order, with no driver's license, often indicate that the individual is not a real person, but rather a fraudulent persona used for illicit purposes. Persons whose names are associated with an address for shipping, but for whom there are no additional records, also indicate the individual is not a real person, but rather an alias used to conceal the name of the real recipient of the shipment. For all these above reasons, I believe "Larry Alexandra," "Alexandra Alomari," and "Matthew Quinn," are not actual people, but just aliases used by MACKMORE to distance himself from evidence of his crimes.

Undercover Texting with MACKMORE

11. From December 27, 2023, to January 3, 2023, I, acting as an Undercover Agent ("UCA"), had an undercover text messaging conversation with MACKMORE, 217-994-7002, that included the following:

12/27/2023

UCA:

"you have teslins?" [Teslins are a plastic substrate used within identification cards to make security features such as seals that are tamper-resistant. Because they are used in genuine identification cards, they are also a hallmark of quality counterfeit cards]

7002:

"what kind u need"

UCA:

"PA and AZ to starting. What u price?"

"also bro u get holo [hologram] overlays also?"

7002:

"Yea"

UCA:

"great what u price? If is quality good then I will pay for it is good"

12/28/2023

UCA:

"bro? u got?"

1/3/2024

7002:

"bro"

"if u want the plug [slang for top provider of black market goods] I'm gon plug u 400 tho let me no"

UCA:

"Dam bro u up early. Yah I still need what I be getting for 400? Also bro u just make dls [driver's licenses] good quality. what u charging for that?"

7002:

"what u need Hml [Hit my line, i.e., contact me directly]"

UCA:

"if u good quality we needing 10 dls each month. Not I care what state if they good quality. I will pay good money for good quality bro. Also if this good I have lot of friends will be needing a lot"

7002:

"Ok"

Neither MACKMORE Nor KELLY Has a Job That Would Support Their Lifestyle

12. I spoke with an investigator from the California Employment Development Department, which is responsible for tracking wage data in California, and he told me there was no record of MACKMORE or KELLY receiving wages since at least January 2020.

Search Warrant Served at MACKMORE's Residence

13. On January 29, 2024, the Honorable Charles F. Eick signed a search warrant for MACKMORE's residence, 1100 W Temple St, Apt 611, Los Angeles, CA (2:24-MJ-00459). On January 31, 2024, I, and other officers, served the search warrant at MACKMORE's residence. Present at the residence at the time of the warrant was: MACKMORE, KELLY, and MACKMORE's adult son, Rashee WASHINGTON.

14. The search of MACKMORE's residence resulted in the seizure of the following items among others:

a. 8 partially completed counterfeit credit cards (with

some account information printed)

b. *6 counterfeit credit card blanks (with bank logos/branding but no account information)*

c. *30 counterfeit driver's licenses (MI, PA, SC)*

d. *249 counterfeit MI driver's licenses (printed, pre-laminate)*

e. *56 counterfeit PA driver's licenses (printed, pre-laminate)*

f. *4 counterfeit MI driver's license Teslin security features*

g. *4 counterfeit PA driver's license Teslin security features*

h. *3 counterfeit IL driver's license Teslin security features*

i. *367 credit card blanks (with mag stripe, no branding or account info)*

j. *18 identification card blanks (with mag stripe)*

k. *8 PVC card blanks (ID or CC, no mag stripe)*

l. *134 id card laminates*

m. *70 laminate sheets (8 ½ x 11)*

n. *4 blank teslin sheets (8 ½ x 11)*

o. *900 blank checks (no account info)*

p. *50 blank checks (Bank of America, account: xxxxxxx2828)*

q. *Correspondence for: MACKMORE, KELLY, Larry Alexandra, James Campbell, Anita Washington, David Robinson, R&P Trucking, and M&M logistics*

r. *1 genuine birth certificate (Justine Zesati)*

s. *Notebooks containing personal identifying information and/or financial information for at least 70 individuals (not MACKMORE or KELLY): (info includes: names, DOB, SSN, bank account numbers, usernames,*

passwords, addresses, emails, and phone numbers).

15. The counterfeit driver's licenses described above contained the photographs of MACKMORE, KELLY, WASHINGTON, and at least twenty other individuals.

Review of Digital Evidence seized from MACKMORE

16. The review of MACKMORE's cellular telephone and seizure of relevant evidence, revealed the following information:

a. MACKMORE's phone contained photos of himself (selfies), his apartment, counterfeit identifications, counterfeit access device cards, partially completed counterfeit identifications, computer software being used to manufacture counterfeit identifications, account information belonging to other people, personal identifiable information belonging to other people, counterfeit checks, checks belonging to other people, and fraudulent identification security features.

b. Photos, videos, and messaging on MACKMORE's phone showed that he was engaged in the following fraud activities during the following time periods: 9/2020 unemployment claims, 11/2020 manufacturing credit cards, 12/2020 manufacturing fraudulent identifications, 12/2020 check fraud, 6/2021 fraudulent access of bank accounts, 7/2022 check fraud, 7/2022 fraudulent access of bank accounts, and 10/2022 credit card fraud.

c. MACKMORE's phone showed that most recently he had engaged in the unauthorized access of victims' cellular telephone accounts (such as Apple, AT&T, and T-mobile), for the

purpose of acquiring merchandise (such as cell phones, tablets, and ear pods) using the victims' credit, which MACKMORE would then re-sell for cash. MACKMORE had engaged in the fraud scheme since at least March 2023, up to January 2024. MACKMORE obtained the stolen account credentials from sellers on Telegram (a messaging and communication platform). Each victim's account obtained by MACKMORE could be used to fraudulently obtain between 1 to 5 devices. Just from September 22, 2023, through October 17, 2023, MACKMORE obtained at least 33 victims' accounts. When accessing unauthorized victim accounts, MACKMORE would manufacture fraudulent identifications containing the victim's information, but with a photograph of a suspect working for MACKMORE, who would be physically receiving merchandise at a store, using the victim's account.

d. MACKMORE's phone contained numerous videos and photographs of firearms. Many of the images depicted firearms, but often the identity of the holder of the firearm could not be determined. Two photos, dated 10/2/23 and 12/20/23, depicted MACKMORE holding a Glock 19 handgun and the metadata for the photos states that they were taken in Los Angeles County. One photo, dated 12/23/23, depicted MACKMORE driving a vehicle, with a second male in the backseat holding a handgun. Two videos, dated 5/23/2022 and 5/30/2022, depicted MACKMORE holding a handgun.

17. The review and seizure of relevant evidence, from a Gateway Laptop seized at the warrant on MACKMORE's residence revealed various identification and credit card making evidence,

to include: fraudulent identification templates, completed, and partially completed fraudulent identifications, counterfeit credit card blanks, identification photographs, identification and credit card photoshop files, and barcodes.

MACKMORE's Confession

18. On January 31, 2024, in the course of the search warrant on MACKMORE's residence, I and SA Cristian Saenz interviewed MACKMORE. Prior to the interview beginning I identified myself and informed MACKMORE that he was not under arrest and was free to leave at any time. I also interviewed MACKMORE in a portion of the residence where no one was impeding his ability to leave the residence if he so chose. MACKMORE stated that he understood and agreed to talk to me and SA Saenz. In the course of the interview the following pertinent statements occurred:

a. MACKMORE has resided at the residence since it opened for at least two years. MACKMORE's fiancé, Precious KELLY, also resides there, and his son Rashee WASHINGTON is currently staying with them at the residence as well.

b. MACKMORE said that anything illegal found in the apartment belonged to him, and did not belong to KELLY or WASHINGTON. I directed MACKMORE's attention to a shelf containing more than twenty counterfeit driver's licenses, asking if MACKMORE's ownership included the driver's licenses, to which MACKMORE said yes.

c. MACKMORE identified two cellular telephones in the apartment belonging to him.

d. MACKMORE stated that he has been purchasing counterfeit driver's license security features from China for approximately eight months using Telegram and Whatsapp messaging (which are encrypted). MACKMORE says he pays via bitcoin. I directed MACKMORE's attention to a sheet of counterfeit Teslin driver's license security features found in the apartment, asking if these were examples of his purchases, and MACKMORE said they were. I then asked MAKCMORE what state the features were for, to which MACKMORE correctly said PA.

19. I told MACKMORE he would need to retain a criminal defense attorney, telling him that if he did so, he could negotiate a plea agreement without being arrested. I explained to him that to avoid arrest, he needed to stay in contact with me. My last communication with MACKMORE was on May 17, 2024, during which we agreed to talk again shortly. Since May 17, 2024, I have made numerous unanswered phone calls and sent numerous unanswered text messages to MACKMORE and KELLY. Based on the fact that phone calls to MACKMORE immediately go to voicemail I believe his phone is turned off. Furthermore, based on the fact that MACKMORE's voicemail message has changed to an automated message I believe he has changed his phone number entirely.

20. On June 17, 2024, I confirmed with the leasing office for MACKMORE's apartment that MACKMORE no longer resides there, and that he did not leave any forwarding address.

PRECIOUS KELLY

21. Precious Kelly ("KELLY") is MACKMORE's fiancé, who was residing at MACKMORE's apartment at the time of the search warrant. A counterfeit driver's license was seized in the course of the warrant bearing KELLY's photograph. As described in more detail below, KELLY has assisted MACKMORE with his manufacturing of fraudulent identifications and his unauthorized access of victims' cellular telephone accounts scheme since at least January 16, 2023. Digital evidence seized in the course of the search warrant showed that KELLY had engaged in the creation and editing of digital fraudulent identifications for MACKMORE. KELLY also engaged in the printing of fraudulent identifications. She also assisted MACKMORE in various other aspects of the scheme, to include researching the value of fraudulently obtained merchandise, sending images of fraudulent identifications, trying to resolve issues with the printing and manufacturing of fraudulent identifications, and transferring virtual currency for expenses associated with the scheme, as described below.

22. Both MACKMORE and KELLY had confirmed with me during the search warrant their telephone numbers, as well as physically identifying their phones, and providing passcodes. KELLY and MACKMORE had the following pertinent text messaging communications regarding the fraud activity described above:

a. On January 16, 2023, MACKMORE and KELLY have a texting conversation about the manufacturing of a fraudulent identification, First MACKMORE sends KELLY a virtual currency address, to which KELLY sends proof of virtual

currency being sent to the address. Then KELLY sends MACKMORE the barcode for an identification. Then they have a further text conversation including the following pertinent messages:

KELLY: "can u send me a pic of his id"

MACKMORE: "yes"

KELLY: "I have to do so much editing on this pictures they sent you"

Kelly included a photograph of a computer screen depicting a software program being used to create a fraudulent driver's license.

b. On July 11, 2023, MACKMORE messaged KELLY information to make five driver's licenses (name, date of birth, height weight, hair, eyes, and address). To which KELLY replied back "yea." Then on July 13, 2024, MACKMORE sent KELLY a text listing five driver's license state abbreviations, "Tx, Pa, La, IL, FL." To which KELLY replied saying "no La." MACKMORE replied saying to try "TX" instead.

c. On October 3, 2023, MACKMORE and KELLY had a text conversation regarding the printing and manufacturing of more fraudulent identifications, which included the following pertinent texts:

MACKMORE: "can u re print those 2"

KELLY: "K"

KELLY: "your going to need ink"

KELLY: "It's done tho"

MACKMORE: "ok"

MACKMORE: "turn that laminator on"

KELLY: "Ok"

d. On October 4, 2023, MACKMORE and KELLY had a text conversation regarding accessing victim cell phone accounts and obtaining merchandise, the conversation included the following:

MACKMORE: sent a screen shot of two AT&T Victim accounts

KELLY: responded sending screenshots of two AT&T account homescreen logins, texting: "Ya'll good"

MACKMORE: "Yes, lakewood"

KELLY: "ok"

MAKCMORE: "got 2"

23. Since MACKMORE stopped responding to my calls, I have also attempted to located KELLY. KELLY also stopped answering her cellphone at the same time as MACKMORE; furthermore it appears that her cellphone is also no longer active. Additionally, KELLY did not leave any forwarding information or address at her prior address. I also conducted queries of various law enforcement databases to attempt to locate a current address for KELLY, and have not found any addresses listed.

RASHEE WASHINGTON

24. Rashee Washington ("WASHINGTON") is MACKMORE's adult son, and was residing at MACKMORE's apartment at the time of the search warrant. As described in detail below, WASHINGTON has assisted MACKMORE and KELLY with their manufacturing of fraudulent identifications and the unauthorized access of victims' cellular telephone accounts scheme since at least

December 16, 2024. The search warrant resulted in the seizure of 14 fraudulent laminated driver's licenses bearing WASHINGTON's photograph, and an additional 120 unlaminated fraudulent driver's licenses also bearing his photograph. Of the 14 fraudulent laminated driver's licenses, 6 bore the names of victims whose identities MACKMORE had purchased to access their cellular telephone accounts, per text messages discovered on MACKMORE's phone. Thus it appears that MACMORE used his son to impersonate victims to pick up merchandise in their names, for which companies typically require identification. MACKMORE's phone also contained two photographs taken on December 16, 2024, containing stacks of 17 iPads and 18 iPhones. We recovered minimal text messages between MACKMORE and WASHINGTON. On January 15, 2024, however, MACKMORE sent WASHINGTON two photographs, the first was of a Glock handgun with an extended clip, and the second was of MACKMORE holding a stack of cash.

25. MACKMORE and KELLY text messaged regarding the 6 fraudulent identifications bearing victim information and WASHINGTON's photograph. Specifically, on December 16, 2023, MACKMORE sent the 6 stolen account logins to KELLY. Based on prior text conversations between MACKMORE and KELLY, MACKMORE would send stolen account information to KELLY for the purpose of her assisting in the manufacturing of the fraudulent identifications and for checking the status or balance of stolen accounts.

26. Since MACKMORE stopped responding to my calls, I also attempted to located WASHINGTON. WASHINGTON did not leave any forwarding information or address at his prior address. I also conducted queries of various law enforcement databases to attempt to locate a current address for WASHINGTON, and have not found any addresses listed for him.

AT&T Data and Information Obtained

27. I obtained data and information from AT&T regarding MACKMORE, KELLY, and WASHINGTON, as well as victim information recovered in the course of the investigation. My review of that data revealed the following pertinent facts:

a. I had requested records from AT&T regarding a sampling of sixty-nine AT&T stolen account credentials, purchased by MACKMORE, between March 6, 2023, and December 16, 2023. This was not the total number of stolen credentials purchased by MACKMORE but just a sampling. AT&T queried all transactions regarding the stolen accounts. In total there were one hundred and sixty-four (164) fraudulent transactions identified occurring on those stolen accounts. Specifically, there were seventy-four instances of Add-On Fraud for a total of $81,775.40 in device value; twelve instances of Upgrade Fraud for a total of $14,126.91 in device value; and seventy-seven instances of Accessory Fraud for a total of $19,038.24 in device value.

b. I observed that some of the fraudulent transactions described above listed a credit card which was used to pay tax on the fraudulent transactions. Many of the cards

used to pay tax were gift cards or did not bear any name, but I recognized that some of the card holder names on those cards used to pay taxes were: MACKMORE or KELLY.

c. I requested AT&T conduct a further review of other instances of fraud in which a credit card was used to pay tax, bearing the names: MACKMORE or KELLY. AT&T data showed that credit cards bearing KELLY's name used to pay tax on an additional eighty-eight fraudulent transactions with a total value of $27,409.12 in fraudulently obtained merchandise. Further data showed that a credit card bearing MACKMORE's name was used to pay tax on an additional ten fraudulent transactions with a total value of $2,379.90 in fraudulently obtained merchandise.

d. AT&T informed me that they had an open fraud investigation on WASHINGTON as well. Specifically, AT&T had discovered that a Visa gift card had been used to pay the tax on one hundred and fourteen fraudulent transactions throughout southern California, from October 25, 2023, through December 11, 2023, resulting in $22,527.68 of fraudulently obtained merchandise. Although AT&T retail stores do not typically save surveillance camera footage, because of the AT&T investigation into the same gift card used to pay tax on the fraudulent transactions, eight surveillance photos were preserved for different fraudulent transactions. All photos depicted the same individual conducting the fraudulent transactions. The individual depicted is WASHINGTON, but he used the names of victims.

MACKMORE, KELLY, and WASHINGTON Fled from Law Enforcement

28. After I informed MACKMORE that he should hire a criminal defense attorney to negotiate a plea agreement to this conduct, he stopped responding to me and terminated the only telephone number I had for him around March of 2024. I later learned that MACKMORE, KELLY, and WASHINGTON all left the address I had previously found them in during the execution of the search warrant, and none left any forwarding information with the Post Office or the apartment rental company. The telephone numbers I found for KELLY and WASHINGTON during the search warrant were also terminated around the same time, so it appears they made a collective decision to leave and make it difficult to determine their whereabouts. I have run their identifiers through multiple law enforcement databases in an effort to locate them without any success.

MACKMORE, KELLY, and WASHINGTON Use Aliases.

29. This investigation resulted in the seizure of more than three hundred fraudulent identifications, bearing the photographs of MACKMORE, KELLY, and WASHINGTON, as well as other co-conspirators, to include: eighty-six fraudulent identifications bearing MACKMORE's photograph and aliases; one hundred and thirty-four fraudulent identifications bearing WASHINGTON's photograph and aliases; and one fraudulent identification bearing KELLY's photo and an alias.

MACKMORE's use of Firearms

30. The search of MACKMORE's digital devices, revealed photographs and videos of numerous firearms to include photos

and videos depicting him possessing firearms. The photographs of MACKMORE with guns included one with a handgun which had a drum magazine which has a 50 round capacity. Other photographs depicted assault rifles and high capacity magazines.

FEDERAL JURISDICTION

31. In my training and experience, each of the financial institutions mentioned in this affidavit is both federally-insured and operates in interstate commerce, as do the victim telephone companies that were tricked into providing MACKMORE and his conspirators with electronics on credit in the names of victims of identity theft. The evidence seized from the conspirators' residence showed that they submitted by internet, an instrumentality of interstate commerce, their fraudulent applications for electronic devices on credit.

///

CONCLUSION

32. Based on the foregoing facts, there is probable cause to believe that RASHEE MACKMORE, PRECIOUS KELLY, and RASHEE WASHINGTON committed violations of Title 18, United States Code, Sections 1349, 1343, 1344, and 1028A (conspiracy to commit wire and bank fraud, and aggravated identity theft).

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 20th day of December, 2024.

UNITED STATES MAGISTRATE JUDGE